Research Paper | Network Security | E-ISSN No : 2454-9916 | Volume : 9 | Issue : 9 | September 2023

A REVIEW ON DIGITAL SIGANTURE SCHEMES

Shyma Kareem

Assistant Professor, Department of Computer Applications, Musaliar College of Engineering and Technology, Pathanamthitta

ABSTRACT

The most significant progress from the effort on public key cryptography is the digital signature. A digital signature is a scientific scheme for verifying the authenticity of digital messages or documents. It provides message authentication and data integrity. This paper is a survey on existing digital signature schemes used for authentication. The purpose of this review is to bring the idea of digital signature technique for researchers.

KEYWORDS: Digital Signature, RSADSS, EDSS, SDSS, NISTDSS, ECDSS

1. INTRODUCTION

The handwritten signature on a document is used to certify that the signer is answerable for the content of the document. Similarly a digital signature is a technique that binds a person/entity to the digital data [1][10]. This binding can be verified by the receiver. The sender uses a signing algorithm to sign the message/document and receiver uses a verification algorithm to verify it. The signer signs the document with his/her own private key and verifier verifies with signer's public key [2]. The Digital Signature Model is shown in Figure 1.

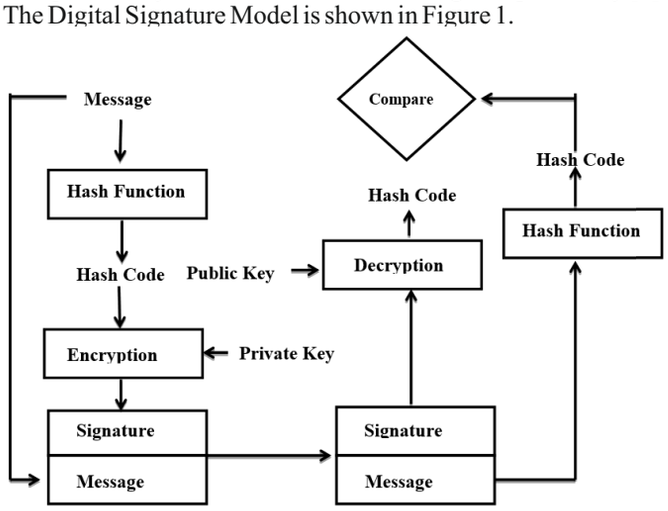

Figure 1: Digital Signature Model

All digital signature schemes are based on public/asymmetric key cryptography. Each user supporting this scheme has a public-private key pair. The private key used for signing is mentioned to as the signature key and the public key as the verification key. The Signer generates hash of data. The hash value and signed key are then fed to the signature algorithm which produces the digital signature on given hash code [3][11]. The signature is then appended to the message and then both are sent to the verifier. The verification algorithm gives some value as output. Verifier also runs same hash function on received message to generate hash value. For the verification process, the newly generated hash value and output of verification algorithm are compared. The verifier decides whether the digital signature is valid or not based on the comparison result.

2. Digital Signature schemes

The schemes which provide a way of signing messages digitally is called digital signature schemes. A digital signature scheme will have two components [4] like Private Signing Algorithm and Public Verification Algorithm. The Private Signing Algorithm is used for creating Digital Signature by using private key. The Public Verification Algorithm is used for Verifying the Digital Signature created by the sender. There are many digital signature schemes which meet these components.

2.1 Elgamal Digital Signature Scheme (EDSS)

The Elgamal digital signature scheme is designed to enable encryption by user's public key and enable decryption by user's private key. It was described by Taher Elgamal in 1985. It is based on the difficulty of computing Discrete logarithms. The Elgamal Digital Signature Scheme includes the following procedures.

Procedure 1: Global Domain Parameters

- q – a prime number
- α – primitive root of q

Procedure 2: Key Generation

1. User A generate the key pair – Generate a random integer X_A such that $1< X_A <q-1$
2. Compute $Y_A=\alpha^{X_A} \bmod q$
3. A's private key is X_A
4. A's public key is $\{q,\alpha,Y_A\}$

To sign a message M ,user A first computes the hash m = H(M),such that m is an integer in range $0 \leq m \leq q-1$

Procedure 3: Signing

1. Choose a random integer K such that $1 \leq K \leq q-1$ and GCD (K,q-1)=1
2. Compute $S1=\alpha^K \bmod q$
3. Compute $K^{-1} \bmod (q-1)$
4. Compute $S2=K^{-1}(M-XAS1) \bmod (q-1)$
5. Signature=(S1,S2)

Procedure 4: Verification

1. Compute $V1 = \alpha^M \bmod q$
2. Compute $V2 = (YA)^{S1} (S1)^{S2} \bmod q$
3. If V1 = V2 signature is valid

2.2 Schnorr Digital Signature Scheme (SDSS)

This signature scheme is based on discrete logarithms [6]. It minimizes the message dependent amount of computation required to generate a signature [5]. It was developed by Claus Schnorr. It is a scheme known for its simplicity. The Schnorr Digital Signature Scheme includes the following procedures.

Procedure 1: Global Domain Parameters

- Choose prime numbers p and q such that q is a prime factor of p-1
- Choose an integer α such that $\alpha^q = 1 \bmod p$

Procedure 2: Key Generation

1. Choose a random integer s as user's private key such that $0 < s < q$.
2. Calculate $V = \alpha^{-s} \bmod p$. This is user's public key.

Procedure 3: Signing

1. Choose a random integer r with $0 < r < q$ and compute $x = \alpha^r \bmod p$.
2. Compute $e = H(M||x)$
3. Compute $y = (r+se) \bmod q$.
4. Signature = (e,y)

Procedure 4: Verification

1. Compute $x' = \alpha^y v^e \bmod p$
2. Verify that $e = H(M||x')$

2.3 RSA Digital Signature Scheme

The concept of RSA is based on the product of two large prime numbers which are difficult to factorize. RSA signature scheme is one of the simple digital signature scheme [2][7]. Ron Rivest, Adi Shamir, Len Adleman invented the RSA algorithm which could be used to produce primitive Digital Signature. The RSA Digital Signature Scheme includes the following procedures.

Procedure 1: Global Domain Parameters

- Choose two prime numbers p and q

Procedure 2: Key Generation

1. Compute $n = p*q$ and $Ø = (p-1)*(q-1)$
2. Select a random integer e, $1 < e < Ø$ such that gcd (e, Ø)=1
3. Compute d such that $ed \equiv I \bmod Ø$
4. Public key is e and private key is d

Procedure 3: Signing

1. Compute m=H(M)
2. Compute $s=(m)d \bmod n$
3. Signature=s

Procedure 4: Verification

1. Compute $v = s^e \bmod n$
2. Verify v = m

2.4 NIST Digital Signature Scheme

The NIST Digital signature scheme makes use of secure hash algorithm. The hash code is provided as input to the signature function along with a random number generated for particular signature. The signature function also depends on the sender's private key and a set of parameters known to a group of communicating principles [5][9]. The NIST Digital Signature Scheme includes the following procedures.

Procedure 1: Global Domain Parameters

- p – a prime number where $2^{L-1} < p < 2^L$ for $512 \le L \le 1024$ and L is a multiple of 64
- q – prime divisor of (p-1) where $2^{N-1} < q < 2^N$
- g = h (p-1) /q mod p where h is any integer with $1 < h < (p-1)$ such that $h^{(p-1)}/q \bmod p > 1$

Procedure 2: Key Generation

1. Select x as a private key such that $1 < x < q$
2. Calculate public key $y = g^x \bmod p$
3. Select a pseudo random integer with $0 < k < q$

Procedure 3: Signing

1. Calculate $r = (g^k \bmod p) \bmod q$
2. Calculate $s = (k^{-1} H(M)+xr) \bmod q$
3. Signature = (r,s)

Procedure 4: Verification

1. Calculate $w = (s')^{-1} \bmod q$
2. Calculate u1 = (H(M'))w mod q // M' – received version of original Message M
3. Calculate u2 = (r')w mod q // r'- received version of r
4. Calculate $v = ((g^{u1} y^{u2}) \bmod p) \bmod q$
5. If v = r' verify the signature

2.5 Elliptic Curve Digital Signature Scheme(ECDSS)

This scheme is based on Ellipticcurve cryptography. All participants in this digital signature scheme use the same global domain parameters which define an elliptic curve and a point of origin on the curve [4][8]. The Elliptic Curve Digital Signature Scheme includes the following procedures.

Procedure 1: Global Domain Parameters

- q – a prime number
- a,b – integers that specify the elliptic curve equation defined over z_q with the equation $y^2 = x^3 + ax + b$
- G – a base point represented by $G = (x_g, y_g)$ on the elliptic curve equation
- n – order of point G ie, n is the smallest positive integer such that nG = 0

Procedure 2: Key Generation

1. Select a random integer d such that $d \in [1,n-1]$ as the private key.
2. Compute the public key Q = dG. This is a point in $E_q(a,b)$

Procedure 3: Signing

1. Select a random integer k, such that $k \in [1,n-1]$
2. Compute the point p = (x,y) = kG
3. Calculate r = x mod n , go to step 1 if r=0
4. Compute $t = k^{-1} \bmod n$
5. Compute e = H(M)
6. Compute $s = k^{-1} (e+dr) \bmod n$, go to step 1 if s=0
7. Signature = (r,s)

Procedure 4: Verification

1. Verify r and s are integers in the range 1 through n-1
2. Compute e = H(M)
3. Compute $w = s^{-1} \bmod n$
4. Compute u1 = e*w
5. Compute u2 = r*w
6. Compute the point $X = (x_1, y_1) = u1G + u2Q$
7. If X = 0, reject the signature else compute $v = (x_1) \bmod n$
8. Accept if and only if v = r

3. Comparison of Digital Signature Schemes.

The comparison of different digital signature schemes are shown in Table 1.

Digital Signature Schemes	EDSS	SDSS	RSADSS	NISTDSS	ECDSS
Methods used for Security	Algebraic properties of modular exponentiation together with discrete logarithm	Discrete logarithms.	RSA algorithm.	Discrete logarithms and Secure Hash algorithm	Elliptic curve cryptography

Table1 : Comparison of different schemes

4. Conclusion

Digital Signature is a mathematical method used to validate authenticity and integrity of message, digital documents or software. It is also known as electronic signature. Industries use digital signature technology to streamline processes and improve document integrity. There are many schemes used for the creation of digital signatures. In this paper different types of digital signature schemes and its processing procedures are discussed.

5. REFERENCES

1. F.Li& M.,Khurram Khan ,"A biometric identity based Encryption scheme" Elsevier Future Generation Computer Systems 2010.
2. DraganVidakovic, DuskoParezanovic, OliveraNikolic and JelenaKaljevic, "RSA Signature: Behind the Scenes" Advanced Computing: An International Journal (ACIJ), Vol.4, No.2, March 2013.
3. D.Vidakovic, O. Nikolic, D. Parezanovic, "Acceleration Detection of Large (Probably) Prime Numbers", International Journal of UbiComp (IJU), Vol.4, No.1, January 2013.
4. Hung-Zih Liao and Yuan-Yuan Shen ,"On the Elliptic Curve Digital Signature Algorithm" Tunghai Science Vol. 8,pp.109−126 , July 2006.
5. MihirBellare and Phillip Rogaway , "The Exact Security of Digital Signatures- How to Sign with RSA and Rabin" U. Maurer (Ed.): Advances in Cryptology - EUROCRYPT '96, LNCS 1070, pp. 399-416, 1996. Springer-Verlag Berlin Heidelberg 1996.
6. Shivendra Singh Md. SarfarazIqbal and ArunimaJaiswal ,"Survey on Techniques Developed using Digital Signature: Public key Cryptography", International Journal of Computer Applications (0975 – 8887) Vol. 117 , No. 16, May 2015.
7. Felten EW, Balfanz D, Dean D, Wallach DS. ,"Web spoofing: an internet con game", Software World. 1997; 28(2):6-8.
8. Payal Saha."A comprehensive study on Digital Signature for internet security". ACCENTS Transactions on Information Security , May 2016.
9. L.,Buttyán, L.,Dóra, F.,Martinelli, M.,Petrocchi. "Fast certificate-based authentication scheme in multioperator maintained wireless mesh networks" Elsevier Computer Communications. May 2010.
10. M. Bishop, Introduction to Computer Security, Reading, MA:Addison-Wesley, 2005.
11. W. Stallings, Cryptography and Network Security, NJ:Prentice-Hall, 2015.